The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

The vulnerabilities are based on the CVE vulnerability naming standard and are organized according to severity, determined by the Common Vulnerability Scoring System (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

## High Vulnerabilities

| Primary Vendor -- Product | Description | Discovered Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| ArcSoft -- MMS Composer | Multiple buffer overflows in ArcSoft MMS Composer 1.5.5.6, and possibly earlier, and 2.0.0.13, and possibly earlier, allow remote attackers to cause a denial of service (crash) or execute arbitrary code via crafted MMS (Multimedia Messaging Service) messages that trigger the overflows in the (1) M-Notification.ind, (2) M-Retrieve.conf (Header and Body), or (3) SMIL parsers. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4131<br>BUGTRAQ<br>FULLDISC<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA |
| Bob Jewell -- Discloser | Multiple PHP remote file inclusion vulnerabilities in Bob Jewell Discloser 0.0.4 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the fileloc parameter to (1) content/content.php or (2) /inc/indexhead.php. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4207<br>OTHER-REF<br>OTHER-REF<br>BID<br>XF |
| Boite de News -- Boite de News | PHP remote file inclusion vulnerability in boitenews4/index.php in Boite de News 4.0.1 allows remote attackers to execute arbitrary PHP code via a URL in the url_index parameter. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4123<br>Milw0rm<br>BID<br>XF |
| Chaussette -- Chaussette | Multiple PHP remote file inclusion vulnerabilities in Chaussette 080706 and earlier allow remote attackers to execute arbitrary PHP code via a URL in the _BASE parameter to (1) Classes/Evenement.php, (2) Classes/Event.php, (3) Classes/Event_for_month.php, (4) Classes/Event_for_week.php, (5) Classes/My_Log.php, and (6) Classes/My_Smarty.php. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4159<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA |
| Chaussette -- Chaussette | PHP remote file inclusion vulnerability in Chaussette 080706 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the _BASE parameter to Classes/Event_for_month_per_day.php, a different vector than CVE-2006-4159. NOTE: the provenance of this information is unknown; the details are obtained from third party information. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4216<br>SECUNIA |
| Cisco -- PIX Firewall | ** DISPUTED ** Unspecified vulnerability in Cisco PIX 500 Series Security Appliances allows remote attackers to send arbitrary UDP packets to intranet devices via unspecified vectors involving Session Initiation Protocol (SIP) fixup commands, a different issue than CVE-2006-4032. NOTE: the vendor, after working with the researcher, has been unable to reproduce the issue. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4194<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>CISCO |
| CPG-Nuke -- Dragonfly CMS | Cross-site scripting (XSS) vulnerability in Dragonfly CMS 9.0.6.1 and earlier allows remote attackers to inject arbitrary web script or HTML via the search field. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4162<br>BUGTRAQ<br>XF |
| David Kent Norman -- Thatware | PHP remote file inclusion vulnerability in config.php in David Kent Norman Thatware 0.4.6 and possibly earlier allows remote attackers to execute arbitrary PHP code via a URL in the root_path parameter. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4213<br>OTHER-REF<br>FRSIRT<br>XF |
| DConnect -- DConnect Daemon | Stack-based buffer overflow in main.c in DConnect Daemon 0.7.0 and earlier allows remote attackers to execute arbitrary code via a large nickname, which is not properly handled by the listen_thread_udp function. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4125<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK |

| | | | | |
|---|---|---|---|---|
| | | | | SECUNIA<br>XF |
| Dolphin -- Dolphin | Multiple PHP remote file inclusion vulnerabilities in Dolphin 5.1 allow remote attackers to execute arbitrary PHP code via a URL in the dir[inc] parameter in (1) index.php, (2) aemodule.php, (3) browse.php, (4) cc.php, (5) click.php, (6) faq.php, (7) gallery.php, (8) im.php, (9) inbox.php, (10) join_form.php, (11) logout.php, (12) messages_inbox.php, and many other scripts. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4189<br>SECTRACK<br>XF |
| Drupal -- Job Search | SQL injection vulnerability in the Job Search module (job.module) 4.6 before revision 1.3.2.1 in Drupal allows remote attackers to execute arbitrary SQL commands via a job or resume search. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4107<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Drupal -- Bibliography Module | SQL injection vulnerability in Bibliography (biblio.module) 4.6 before revision 1.1.1.1.4.11 and 4.7 before revision 1.13.2.5 for Drupal allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4108<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA |
| Falko Timme and Till Brehm -- SQLiteWebAdmin | PHP remote file inclusion vulnerability in tpl.inc.php in Falko Timme and Till Brehm SQLiteWebAdmin 0.1 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the conf[classpath] parameter. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4102<br>OTHER-REF<br>FRSIRT<br>XF |
| HP -- OpenView Storage Data Protector | Unspecified vulnerability in the backup agent and Cell Manager in HP OpenView Storage Data Protector 5.1 and 5.5 before 20060810 allows remote attackers to execute arbitrary code on an agent via unspecified vectors related to authentication and input validation. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4201<br>OTHER-REF<br>HP<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>XF |
| IBM -- Informix Dynamic Database Server | Buffer overflow in IBM Informix Dynamic Server (IDS) 9.40.TC7, 9.40.TC8, 10.00.TC4, and 10.00.TC5, when running on Windows, allows remote attackers to execute arbitrary code via a long username, which causes an overflow in vsprintf when displaying in the resulting error message. NOTE: this issue is due to an incomplete fix for CVE-2006-3853. | unknown<br>2006-08-16 | 7.0 | CVE-2006-3854<br>BUGTRAQ<br>BUGTRAQ<br>OTHER-REF |
| IBM -- Websphere Application Server | Multiple unspecified vulnerabilities in IBM WebSphere Application Server before 6.1.0.1 have unspecified impact and attack vectors involving (1) "SOAP requests and responses", (2) mbean, (3) ThreadIdentitySupport, and possibly others. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4136<br>OTHER-REF<br>AIXAPAR<br>AIXAPAR<br>AIXAPAR<br>BID<br>FRSIRT<br>SECUNIA |
| IBM -- Access Support eGatherer ActiveX control | Stack-based buffer overflow in the IBM Access Support eGatherer ActiveX control before 3.20.0284.0 allows remote attackers to execute arbitrary code via a long filename parameter to the RunEgatherer method. | unknown<br>2006-08-18 | 7.0 | CVE-2006-4221<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA |
| Invision Power Services -- Invision Power Board | Unspecified vulnerability in func_topic_threaded.php (aka threaded view mode) in Invision Power Board (IPB) before 2.1.7 21013.60810.s allows remote attackers to "access posts outside the topic." | unknown<br>2006-08-16 | 7.0 | CVE-2006-4155<br>OTHER-REF<br>FRSIRT<br>SECUNIA |
| Jason Alexander -- phNNTP | PHP remote file inclusion vulnerability in article-raw.php in Jason Alexander phNNTP 1.3 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the file_newsportal parameter. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4103<br>BUGTRAQ<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Joomla! -- Webring Component | PHP remote file inclusion vulnerability in admin.webring.docs.php in the Webring Component (com_webring) 1.0 and earlier for Joomla! allows remote attackers to execute arbitrary PHP code via a URL in the component_dir parameter. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4129<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA |
| Microsoft -- Windows Help File Viewer | Multiple unspecified vulnerabilities in Microsoft Windows Help File viewer (winhlp32.exe) allow user-assisted attackers to execute arbitrary code via crafted HLP files. | 2006-07-20<br>2006-08-14 | 8.0 | CVE-2006-4138<br>BUGTRAQ<br>BUGTRAQ<br>BID |

| | | | | |
|---|---|---|---|---|
| Microsoft -- Internet Explorer | Microsoft Internet Explorer 6.0 SP1 and possibly other versions allows remote attackers to cause a denial of service and possibly execute arbitrary code by instantiating COM objects as ActiveX controls, including (1) imskdic.dll (Microsoft IME), (2) chtskdic.dll (Microsoft IME), and (3) msoe.dll (Outlook), which leads to memory corruption. NOTE: it is not certain whether the issue is in Internet Explorer or the individual DLL files. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4193<br>BUGTRAQ<br>BUGTRAQ<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>BID<br>BID<br>BID |
| Microsoft -- Internet Explorer | The Terminal Services COM object (tsuserex.dll) allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code by instantiating it as an ActiveX object in Internet Explorer 6.0 SP1 on Microsoft Windows 2003 EE SP1 CN. | unknown<br>2006-08-18 | 7.0 | CVE-2006-4219<br>BUGTRAQ<br>OTHER-REF<br>BID |
| MODPlug -- Tracker | Multiple buffer overflows in MODPlug Tracker (OpenMPT) 1.17.02.43 and earlier and libmodplug 0.8 and earlier allow user-assisted remote attackers to execute arbitrary code via (1) long strings in ITP files used by the CSoundFile::ReadITProject function in soundlib/Load_it.cpp and (2) crafted modules used by the CSoundFile::ReadSample function in soundlib/Sndfile.cpp, as demonstrated by crafted AMF files. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4192<br>BUGTRAQ<br>OTHER-REF<br>FRSIRT<br>SECUNIA<br>XF<br>XF |
| MusicBrainz -- libmusicbrainz<br>MusicBrainz -- libmusicbrainz SVN | Multiple buffer overflows in libmusicbrainz (aka mb_client or MusicBrainz Client Library) 2.1.2 and earlier, and SVN 8406 and earlier, allow remote attackers to cause a denial of service (crash) or execute arbitrary code via (1) a long Location header by the HTTP server, which triggers an overflow in the MBHttp::Download function in lib/http.cpp; and (2) a long URL in RDF data, as demonstrated by a URL in an rdf:resource field in an RDF XML document, which triggers overflows in many functions in lib/rdfparse.c. | unknown<br>2006-08-17 | 8.0 | CVE-2006-4197<br>BUGTRAQ<br>BID<br>SECTRACK<br>SECUNIA<br>XF<br>XF |
| MVCnPHP -- MVCnPHP | Multiple PHP remote file inclusion vulnerabilities in Tony Bibbs and Vincent Furia MVCnPHP 3.0 allow remote attackers to execute arbitrary PHP code via a URL in the glConf[path_library] parameter to (1) BaseCommand.php, (2) BaseLoader.php, and (3) BaseView.php. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4160<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA |
| myWebland -- miniBloggie | ** DISPUTED ** PHP remote file inclusion vulnerability in cls_fast_template.php in myWebland miniBloggie 1.0 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the fname parameter. NOTE: another researcher was unable to find a way to execute code after including it via a URL. CVE analysis as of 20060816 was inconclusive. | 2006-05-01<br>2006-08-16 | 7.0 | CVE-2006-4163<br>BUGTRAQ<br>BUGTRAQ<br>BID |
| ncompress -- ncompress | The decompress function in compress42.c in (1) ncompress 4.2.4 and (2) liblzw allows remote attackers to cause a denial of service (crash), and possibly execute arbitrary code, via crafted data that leads to a buffer underflow. | unknown<br>2006-08-14 | 7.0 | CVE-2006-1168<br>OTHER-REF<br>DEBIAN<br>MANDRIVA<br>FRSIRT<br>SECUNIA<br>SECUNIA<br>SECUNIA |
| NetCommons -- NetCommons | Cross-site scripting (XSS) vulnerability in NetCommons 1.0.8 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4165<br>JVN<br>BID<br>SECUNIA<br>XF |
| Pearlabs -- Mafia MoBlog | ** DISPUTED ** PHP remote file inclusion vulnerability in big.php in pearlabs mafia moblog 6 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the pathtotemplate parameter. NOTE: a third party claims that the researcher is incorrect, because template.php defines pathtotemplate before big.php uses pathtotemplate. CVE has not verified either claim, but during August 2006, the original researcher has made several significant errors regarding this bug type. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4156<br>BUGTRAQ<br>BID |
| PHPMyRing -- PHPMyRing | SQL injection vulnerability in view_com.php in Nicolas Grandjean PHPMyRing 4.2.0 and earlier allows remote attackers to execute arbitrary SQL commands via the idsite parameter. | 2006-08-09<br>2006-08-14 | 7.0 | CVE-2006-4114<br>Milw0rm<br>BID<br>FRSIRT<br>SECUNIA |
| phpPrintAnalyzer -- phpPrintAnalyzer | PHP remote file inclusion vulnerability in inc/header.inc.php in phpPrintAnalyzer 1.2 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the ficStyle parameter. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4164<br>Milw0rm<br>BID<br>FRSIRT<br>XF |

| | | | | |
|---|---|---|---|---|
| Ruby on Rails -- Ruby on Rails | Ruby on Rails before 1.1.5 allows remote attackers to execute Ruby code with "severe" or "serious" impact via a File Upload request with an HTTP header that modifies the LOAD_PATH variable, a different vulnerability than CVE-2006-4112. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4111<br>RUBY ON RAILS<br>GENTOO<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA |
| Ruby on Rails -- Ruby on Rails | Unspecified vulnerability in the "dependency resolution mechanism" in Ruby on Rails 1.1.0 through 1.1.5 allows remote attackers to execute arbitrary Ruby code via a URL that is not properly handled in the routing code, which leads to a denial of service (application hang) or "data loss," a different vulnerability than CVE-2006-4111. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4112<br>RUBY ON RAILS<br>GENTOO<br>CERT-VN<br>BID<br>SECUNIA<br>SECUNIA<br>XF |
| SAP Software -- Internet Graphics Server | Buffer overflow in SAP Internet Graphics Service (IGS) 6.40 and earlier, and 7.00 and earlier, allows remote attackers to cause a denial of service (crash) or execute arbitrary code via crafted HTTP requests. NOTE: This information is based upon a vague initial disclosure. Details will be updated after the grace period has ended. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4133<br>BUGTRAQ<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA |
| Simple One-File Guestbook -- Simple One-File Guestbook | Simple one-file guestbook 1.0 and earlier allows remote attackers to bypass authentication and delete guestbook entries via a modified id parameter to guestbook.php. | 2006-08-08<br>2006-08-14 | 7.0 | CVE-2006-4122<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Soft3304 -- 04WebServer | Cross-site scripting (XSS) vulnerability in Soft3304 04WebServer 1.83 and earlier allows remote attackers to inject arbitrary web script or HTML via the URL, which is not properly sanitized before it is returned in an error page, a different vulnerability than CVE-2004-1512. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4199<br>OTHER-REF<br>BID<br>SECUNIA<br>XF |
| Soft3304 -- 04WebServer | Unspecified vulnerability in 04WebServer 1.83 and earlier allows remote attackers to bypass user authentication via unspecified vectors related to request processing. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4200<br>OTHER-REF<br>BID<br>SECUNIA<br>XF |
| TinyWebGallery -- TinyWebGallery | PHP remote file inclusion vulnerability in TinyWebGallery 1.5 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the image parameter to (1) image.php or (2) image.php2. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4166<br>BUGTRAQ<br>Milw0rm<br>SECTRACK<br>XF |
| Vincent Hor -- Calendarix | ** DISPUTED ** PHP remote file inclusion vulnerability in cal_config.inc.php in Calendarix 0.7.20060401 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the calpath parameter. NOTE: this issue has been disputed by a third party, who says that the affected $calpath variable is set to a constant value in the beginning of the script. CVE concurs that the initial report is invalid. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4135<br>BUGTRAQ<br>BUGTRAQ<br>MLIST<br>XF |
| VWar -- Virtual War | SQL injection vulnerability in news.php in Virtual War (VWar) 1.5.0 and earlier allows remote attackers to execute arbitrary SQL commands via the (1) sortby and (2) sortorder parameters. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4141<br>BUGTRAQ<br>XF |
| VWar -- Virtual War | SQL injection vulnerability in extra/online.php in Virtual War (VWar) 1.5.0 R14 and earlier allows remote attackers to execute arbitrary SQL commands via the n parameter. | unknown<br>2006-08-14 | 7.0 | CVE-2006-4142<br>BUGTRAQ<br>BID<br>XF |
| WebDynamite -- ProjectButler | Multiple PHP remote file inclusion vulnerabilities in WebDynamite ProjectButler 0.8.4 allow remote attackers to execute arbitrary PHP code via a URL in the rootdir parameter to /classes/ scripts including (1) Cache.class.php, (2) Customer.class.php, (3) Performance.class.php, (4) Project.class.php, (5) Representative.class.php, (6) User.class.php, or (7) common.php. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4205<br>OTHER-REF<br>BID<br>XF |
| WEBInsta -- CMS | PHP remote file inclusion vulnerability in index.php in WEBInsta CMS 0.3.1 and possibly earlier allows remote attackers to execute arbitrary PHP code via a URL in the templates_dir parameter. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4196<br>BUGTRAQ<br>ECHO<br>Milw0rm<br>BID<br>FRSIRT |

| | | | | |
|---|---|---|---|---|
| | | | | SECUNIA |
| WEBInsta -- Mailing List Manager | PHP remote file inclusion vulnerability in install3.php in WEBInsta Mailing List Manager 1.3e allows remote attackers to execute arbitrary PHP code via a URL in the cabsolute_path parameter. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4209<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>XF |
| YaBB -- YaBB SE | Cross-site scripting (XSS) vulnerability in index.php in Yet another Bulletin Board (YaBB) allows remote attackers to inject arbitrary web script or HTML via the categories parameter. | unknown<br>2006-08-16 | 7.0 | CVE-2006-4157<br>BUGTRAQ<br>BID<br>XF |
| Zen Cart -- Zen Cart | Multiple SQL injection vulnerabilities in Zen Cart 1.3.0.2 and earlier allow remote attackers to execute arbitrary SQL commands via (1) GPC data to ipn_get_stored_session, which can be leveraged to modify elements of $_SESSION; and allow remote authenticated users to execute arbitrary SQL commands via (2) a session id within a cookie to whos_online_session_recreate, (3) the quantity field to the add_cart function, (4) an id[] parameter when adding an item to a shopping cart, or (5) a redemption code when checking out. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4214<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA |
| Zen Cart -- Zen Cart | PHP remote file inclusion vulnerability in index.php in Zen Cart 1.3.0.2 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in autoLoadConfig[999][0][loadFile] parameter. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4215<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA |
| Zen Cart -- Zen Cart | Directory traversal vulnerability in Zen Cart 1.3.0.2 and earlier allows remote attackers to include and possibly execute arbitrary local files via directory traversal sequences in the typefilter parameter. | unknown<br>2006-08-17 | 7.0 | CVE-2006-4218<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA |

Back to top

## Medium Vulnerabilities

| Primary<br>Vendor -- Product | Description | Discovered<br>Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| ASPPlayground.NET -- ASPPlayground.NET Forum | Cross-site scripting (XSS) vulnerability in calendar.asp in ASPPlayground.NET Forum Advanced Edition 2.4.5 Unicode allows remote attackers to inject arbitrary web script or HTML via the calendarID parameter. | unknown<br>2006-08-17 | 4.7 | CVE-2006-4206<br>BUGTRAQ<br>XF |
| b0zz and Chris Vincent -- Owl Intranet Engine | Cross-site scripting (XSS) vulnerability in b0zz and Chris Vincent Owl Intranet Engine 0.90 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown<br>2006-08-17 | 4.7 | CVE-2006-4211<br>OTHER-REF<br>OTHER-REF<br>FRSIRT<br>SECUNIA |
| b0zz and Chris Vincent -- Owl Intranet Engine | SQL injection vulnerability in b0zz and Chris Vincent Owl Intranet Engine 0.90 and earlier allows remote attackers to execute arbitrary SQL commands via unspecified vectors. | unknown<br>2006-08-17 | 4.7 | CVE-2006-4212<br>OTHER-REF<br>OTHER-REF<br>FRSIRT<br>SECUNIA |
| ChaosSoft -- GeheimChaos | Multiple SQL injection vulnerabilities in GeheimChaos 0.5 and earlier allow remote attackers to execute arbitrary SQL commands via the (1) Temp_entered_login or (2) Temp_entered_email parameters to (a) gc.php, and in multiple parameters in (b) include/registrieren.php, possibly involving the (3) $form_email, (4) $form_vorname, (5) $form_nachname, (6) $form_strasse, (7) $form_plzort, (8) $form_land, (9) $form_homepage, (10) $form_bildpfad, (11) $form_profilsichtbar, (12) $Temp_sprache, (13) $form_tag, (14) $form_monat, (15) $form_jahr, (16) $Temp_akt_string, (17) $form_icq, (18) $form_msn, (19) $form_yahoo, (20) $form_username, and (21) $Temp_form_pass variables. | 2006-08-03<br>2006-08-14 | 5.6 | CVE-2006-4118<br>BUGTRAQ<br>FULLDISC<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| ChaosSoft -- GeheimChaos | SQL injection vulnerability in gc.php in GeheimChaos 0.5 and earlier allows remote attackers to execute arbitrary SQL commands via the Temp_entered_password parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information. | unknown<br>2006-08-14 | 5.6 | CVE-2006-4119<br>SECUNIA<br>XF |
| Drupal -- Recipe Module<br>Drupal -- Drupal | Cross-site scripting (XSS) vulnerability in the Recipe module (recipe.module) before 1.54 for Drupal 4.6 and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown<br>2006-08-14 | 5.6 | CVE-2006-4120<br>DRUPAL<br>DRUPAL<br>BID<br>FRSIRT<br>SECUNIA |

| | | | | |
|---|---|---|---|---|
| e-Zest Solutions -- PgMarket | PHP remote file inclusion vulnerability in common.inc.php in PgMarket 2.2.3, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via the CFG[libdir] parameter. | unknown<br>2006-08-14 | 5.6 | CVE-2006-4115<br>BUGTRAQ<br>BID<br>XF |
| Hitweb -- Hitweb | PHP remote file inclusion vulnerability in genpage-cgi.php in Brian Fraval hitweb 4.2 and possibly earlier versions allows remote attackers to execute arbitrary PHP code via the REP_INC parameter. | 2006-08-08<br>2006-08-14 | 5.6 | CVE-2006-4113<br>Milw0rm<br>BID<br>FRSIRT<br>SECUNIA |
| IBM -- Informix Dynamic Database Server | IBM Informix Dynamic Server (IDS) before 9.40.xC7 and 10.00 before 10.00.xC3 allows allows remote authenticated users to execute arbitrary commands via the (1) "SET DEBUG FILE" SQL command, and the (2) start_onpload and (3) dbexp functions. | unknown<br>2006-08-16 | 4.7 | CVE-2006-3860<br>BUGTRAQ<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF<br>XF |
| Lesstif -- Lesstif | The libXm library in LessTif 0.95.0 and earlier allows local users to gain privileges via the DEBUG_FILE environment variable, which is used to create world-writable files when libXm is run from a setuid program. | unknown<br>2006-08-14 | 4.9 | CVE-2006-4124<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Lhaz -- Lhaz | Multiple stack-based buffer overflows in Lhaz before 1.32 allow user-assisted attackers to execute arbitrary code via a long filename in (1) an LHZ archive, when saving the filename during extraction; and (2) an LHZ archive with an invalid CRC checksum, when constructing an error message. | unknown<br>2006-08-14 | 5.6 | CVE-2006-4116<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>FRSIRT<br>SECUNIA<br>XF<br>XF |
| MamboXChange -- PeopleBook | PHP remote file inclusion vulnerability in param.peoplebook.php in the Peoplebook Component for Mambo (com_peoplebook) 1.0 and earlier, and possibly 1.1.2, when register_globals and allow_fopenurl are enabled, allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-17 | 5.6 | CVE-2006-4195<br>BUGTRAQ<br>Milw0rm<br>BID<br>SECUNIA |
| MamboXChange -- Mambo eMail Publisher | PHP remote file inclusion vulnerability in help.mmp.php in the MMP Component (com_mmp) 1.2 and earlier for Mambo allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-17 | 4.7 | CVE-2006-4203<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| Matt Smith -- ReMOSitory for Mambo | PHP remote file inclusion vulnerability in admin.remository.php in the Remository Component (com_remository) 3.25 and earlier for Mambo and Joomla!, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the mosConfig_absolute_path parameter. | unknown<br>2006-08-14 | 5.6 | CVE-2006-4130<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| NetGear -- FVG318 | Netgear FVG318 running firmware 1.0.40 allows remote attackers to cause a denial of service (router reset) via TCP packets with bad checksums. | unknown<br>2006-08-14 | 5.0 | CVE-2006-4143<br>BUGTRAQ<br>BID<br>XF |
| PHP-Nuke -- AutoHTML Module | Directory traversal vulnerability in autohtml.php in the AutoHTML module for PHP-Nuke allows local users to include arbitrary files via a .. (dot dot) in the name parameter for a modload operation. | unknown<br>2006-08-16 | 4.9 | CVE-2006-4190<br>BUGTRAQ<br>OTHER-REF<br>BID |
| PHProjekt -- PHProjekt | Multile PHP remote file inclusion vulnerabilities in PHProjekt 5.1 and possibly earlier allow remote attackers to execute arbitrary PHP code via a URL in the (1) path_pre parameter in lib/specialdays.php and the (2) lib_path parameter in lib/dbman_filter.inc.php. | unknown<br>2006-08-17 | 4.7 | CVE-2006-4204<br>OTHER-REF<br>BID<br>SECUNIA |
| See-Commerce -- See-Commerce | PHP remote file inclusion vulnerability in owimg.php3 in See-Commerce 1.0.625 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the path parameter. | unknown<br>2006-08-14 | 5.6 | CVE-2006-4121<br>OTHER-REF<br>BID<br>FRSIRT |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  |  | SECUNIA |
| Spaminator -- Spaminator | PHP remote file inclusion vulnerability in Login.php in Spaminator 1.7 and earlier allows remote attackers to execute arbitrary PHP code via a URL in the page parameter. | unknown<br>2006-08-16 | 5.6 | CVE-2006-4158<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| SquirrelMail -- SquirrelMail | Dynamic variable evaluation vulnerability in compose.php in SquirrelMail 1.4.0 to 1.4.7 allows remote attackers to overwrite arbitrary program variables and read or write the attachments and preferences of other users. | unknown<br>2006-08-11 | 4.7 | CVE-2006-4019<br>SQUIRRELMAIL<br>SQUIRRELMAIL<br>FRSIRT<br>SECUNIA<br>BUGTRAQ<br>BUGTRAQ<br>FULLDISC<br>MLIST<br>OTHER-REF<br>BID<br>OSVDB<br>SECTRACK<br>SECUNIA<br>XF |
| Symantec Veritas -- Backup Exec | Multiple heap-based buffer overflows in Symantec VERITAS Backup Exec for Netware Server Remote Agent for Windows Server 9.1 and 9.2 (all builds), Backup Exec Continuous Protection Server Remote Agent for Windows Server 10.1 (builds 10.1.325.6301, 10.1.326.1401, 10.1.326.2501, 10.1.326.3301, and 10.1.327.401), and Backup Exec for Windows Server and Remote Agent 9.1 (build 9.1.4691), 10.0 (builds 10.0.5484 and 10.0.5520), and 10.1 (build 10.1.5629) allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted RPC message. | unknown<br>2006-08-14 | 4.2 | CVE-2006-4128<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>XF |
| Wheatblog -- Wheatblog | PHP remote file inclusion vulnerability in includes/session.php in Wheatblog (wB) 1.1 and earlier, when register_globals is enabled, allows remote attackers to execute arbitrary PHP code via a URL in the wb_class_dir parameter. | unknown<br>2006-08-17 | 5.6 | CVE-2006-4198<br>BUGTRAQ<br>SECWATCH<br>Milw0rm<br>SOURCEFORGE<br>BID<br>XF |
| XMB Software -- Extreme Message Board | Directory traversal vulnerability in memcp.php in XMB (Extreme Message Board) 1.9.6 and earlier allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the langfilenew parameter, as demonstrated by injecting PHP sequences into an Apache HTTP Server log file, which is then included by header.php. | unknown<br>2006-08-16 | 5.6 | CVE-2006-4191<br>BUGTRAQ<br>ALTERVISTA<br>Milw0rm<br>BID<br>SECUNIA<br>XF |

Back to top

## Low Vulnerabilities

| Primary<br>Vendor -- Product | Description | Discovered<br>Published | CVSS Score | Source & Patch Info |
|---|---|---|---|---|
| Andreas Kansok -- phPay | nu_mail.inc.php in Andreas Kansok phPay 2.02 and 2.02.1, when register_globals is enabled, allows remote attackers to use the server as an open mail relay via modified mail_text2, user_row[5], nu_mail_1, and shop_mail parameters. NOTE: some of these details are obtained from third party information. | unknown<br>2006-08-17 | 2.3 | CVE-2006-4210<br>OTHER-REF<br>BID<br>SECUNIA<br>XF |
| Apache Software Foundation -- Apache | Apache 2.2.2, when running on Windows, allows remote attackers to read source code of CGI programs via a request that contains uppercase (or alternate case) characters that bypass the case-sensitive ScriptAlias directive, but allow access to the file on case-insensitive file systems. | 2006-08-08<br>2006-08-14 | 1.9 | CVE-2006-4110<br>BUGTRAQ<br>BID<br>FRSIRT<br>SECUNIA |
| Arcsoft -- MMS Composer | ArcSoft MMS Composer 1.5.5.6 and possibly earlier, and 2.0.0.13 and possibly earlier, allow remote attackers to cause a denial of service (resource exhaustion and application crash) via WAPPush messages to UDP port UDP 2948. | unknown<br>2006-08-14 | 2.3 | CVE-2006-4132<br>BUGTRAQ<br>FULLDISC<br>OTHER-REF<br>OTHER-REF<br>OTHER-REF<br>BID<br>SECUNIA |

| | | | | |
|---|---|---|---|---|
| Blursoft -- Blur6ex | Cross-site scripting (XSS) vulnerability in blursoft blur6ex 0.3 allows remote attackers to inject arbitrary web script or HTML via a comment title. | unknown<br>2006-08-14 | 2.3 | CVE-2006-4106<br>BUGTRAQ<br>BID |
| DConnect -- DConnect Daemon | The dc_chat function in cmd.dc.c in DConnect Daemon 0.7.0 and earlier allows remote attackers to cause a denial of service (application crash) by sending a client message before providing the nickname, which triggers a null pointer dereference. | unknown<br>2006-08-14 | 2.3 | CVE-2006-4126<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>XF |
| DConnect -- DConnect Daemon | Multiple format string vulnerabilities in DConnect Daemon 0.7.0 and earlier allow remote administrators to execute arbitrary code via format string specifiers that are not properly handled when calling the (1) privmsg() or (2) pubmsg functions from (a) cmd.user.c, (b) penalties.c, or (c) cmd.dc.c. | unknown<br>2006-08-14 | 3.4 | CVE-2006-4127<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>XF |
| Drupal -- Bibliography Module | Cross-site scripting (XSS) vulnerability in Bibliography (biblio.module) 4.6 before revision 1.1.1.1.4.11 and 4.7 before revision 1.13.2.5 for Drupal allows remote attackers to inject arbitrary web script or HTML via unspecified vectors. | unknown<br>2006-08-14 | 2.3 | CVE-2006-4109<br>DRUPAL<br>BID<br>FRSIRT<br>SECUNIA |
| Fill Threads Database -- Fill Threads Database | Cross-site scripting (XSS) vulnerability in Fill Threads Database (FTD) 3.7.3 allows remote attackers to inject arbitrary web script or HTML via the (1) search field or (2) an e-mail message. | unknown<br>2006-08-14 | 2.3 | CVE-2006-4105<br>BUGTRAQ<br>BID<br>SECTRACK<br>XF |
| Gallery Project -- Gallery | Unspecified vulnerability in the stats module in Gallery 1.5.1-RC2 and earlier allows remote attackers to obtain sensitive information via unspecified attack vectors, related to "two file exposure bugs." | unknown<br>2006-08-16 | 2.3 | CVE-2006-4030<br>OTHER-REF<br>DEBIAN<br>BID<br>FRSIRT<br>SECUNIA<br>SECUNIA |
| High Availability Linux Project -- Heartbeat | The heartbeat subsystem in High-Availability Linux before 1.2.5 and 2.0 before 2.0.7 allows remote attackers to cause a denial of service (crash) via a crafted heartbeat message. | unknown<br>2006-08-16 | 2.3 | CVE-2006-3121<br>OTHER-REF<br>OTHER-REF<br>DEBIAN<br>BID |
| HP -- HP-UX | Unspecified vulnerability in HP-UX B.11.00, B.11.11 and B.11.23, when running in trusted mode, allows local users to cause a denial of service via unspecified vectors. | unknown<br>2006-08-16 | 1.6 | CVE-2006-4187<br>HP<br>BID<br>SECTRACK |
| HP -- HP-UX | Unspecified vulnerability in the LP subsystem in HP-UX B.11.00, B.11.04, B.11.11, and B.11.23 allows remote attackers to cause a denial of service via unknown vectors. | unknown<br>2006-08-16 | 2.3 | CVE-2006-4188<br>HP<br>BID<br>SECTRACK<br>SECUNIA |
| IBM -- Informix Dynamic Database Server | IBM Informix Dynamic Server (IDS) allows remote authenticated users to create and overwrite arbitrary files via the (1) LOTOFILE and (2) trl_tracefile_set functions, and the (3) "SET DEBUG FILE" commands. | unknown<br>2006-08-16 | 1.4 | CVE-2006-3859<br>BUGTRAQ<br>BUGTRAQ<br>OTHER-REF |
| IBM -- Websphere Application Server | IBM WebSphere Application Server before 6.1.0.1 allows attackers to obtain sensitive information via unspecified vectors related to (1) the log file, (2) "script generated syntax on wsadmin command line," and (3) traces. | unknown<br>2006-08-14 | 2.3 | CVE-2006-4137<br>OTHER-REF<br>AIXAPAR<br>AIXAPAR<br>AIXAPAR<br>BID<br>FRSIRT<br>SECUNIA |
| IBM -- Websphere Application Server | Multiple unspecified vulnerabilities in IBM WebSphere Application Server before 6.0.2.13 have unspecified vectors and impact, including (1) an "authority problem" in ThreadIdentitySupport as identified by PK25199, and "Potential security exposure" issues as identified by (2) PK22747, (3) PK24334, (4) PK25740, and (5) PK26123. | unknown<br>2006-08-18 | 2.3 | CVE-2006-4222<br>OTHER-REF<br>FRSIRT<br>SECUNIA |

| | | | | |
|---|---|---|---|---|
| ImageMagick -- ImageMagick | Integer overflow in the ReadSGIImage function in sgi.c in ImageMagick before 6.2.9 allows user-assisted attackers to cause a denial of service (crash) and possibly execute arbitrary code via large (1) bytes_per_pixel, (2) columns, and (3) rows values, which trigger a heap-based buffer overflow. | unknown<br>2006-08-15 | 1.9 | CVE-2006-4144<br>BUGTRAQ<br>OTHER-REF<br>BID<br>SECUNIA |
| IPCheck -- Server Monitor | Directory traversal vulnerability in IPCheck Server Monitor 5.3.2.609 and earlier allows remote attackers to read arbitrary files via modified .. (dot dot) sequences in the URL, including (1) "..%2f" (encoded "/" slash), "..../" (multiple dot), and "..%255c../" (double-encoded "\" backslash). | unknown<br>2006-08-14 | 2.3 | CVE-2006-4140<br>BUGTRAQ<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>XF |
| Linux -- Linux kernel | Race condition between the kfree_skb and __skb_unlink functions in the socket buffer handling in Linux kernel 2.6.9, and possibly other versions, allows remote attackers to cause a denial of service (crash), as demonstrated using the TCP stress tests from the LTP test suite. | unknown<br>2006-08-15 | 2.7 | CVE-2006-2446<br>REDHAT<br>OTHER-REF |
| MojoScripts -- mojoGallery | Cross-site scripting (XSS) vulnerability in admin.cgi in mojoscripts.com mojoGallery allows remote attackers to inject arbitrary web script or HTML via the username parameter. NOTE: the provenance of this information is unknown; the details are obtained from third party information. | unknown<br>2006-08-11 | 2.3 | CVE-2006-4087<br>FRSIRT<br>SECUNIA |
| MojoScripts -- mojoGallery | Cross-site scripting (XSS) vulnerability in admin.cgi in mojoscripts.com mojoGallery allows remote attackers to inject arbitrary web script or HTML via "password input." | unknown<br>2006-08-14 | 2.3 | CVE-2006-4104<br>BUGTRAQ<br>BID<br>FRSIRT<br>SECUNIA |
| Novell -- eDirectory | Unspecified vulnerability in the NCPENGINE in Novell eDirectory 8.7.3.8 allows local users to cause a denial of service (CPU consumption) via unspecified vectors, as originally demonstrated using a Nessus scan. | unknown<br>2006-08-16 | 2.3 | CVE-2006-4185<br>NOVELL<br>BID<br>SECTRACK<br>SECUNIA |
| Novell -- eDirectory | The iManager in eMBoxClient.jar in Novell eDirectory 8.7.3.8 writes passwords in plaintext to a log file, which allows local users to obtain passwords by reading the file. | unknown<br>2006-08-16 | 1.6 | CVE-2006-4186<br>OTHER-REF<br>BID<br>SECTRACK<br>SECUNIA |
| SAP Software -- Internet Graphics Server | Unspecified vulnerability related to a "design flaw" in SAP Internet Graphics Service (IGS) 6.40 and earlier and 7.00 and earlier allows remote attackers to cause a denial of service (service shutdown) via certain HTTP requests. NOTE: This information is based upon a vague initial disclosure. Details will be updated after the grace period has ended. | unknown<br>2006-08-14 | 2.3 | CVE-2006-4134<br>BUGTRAQ<br>FULLDISC<br>OTHER-REF<br>BID<br>FRSIRT<br>SECTRACK<br>SECUNIA<br>XF |
| ScatterChat -- ScatterChat | The cryptographic module in ScatterChat 1.0.x allows attackers to identify patterns in large numbers of messages by identifying collisions using a birthday attack on the custom padding mechanism for ECB mode encryption. | unknown<br>2006-08-17 | 1.9 | CVE-2006-4021<br>BUGTRAQ<br>SCATTERCHAT<br>SCATTERCHAT |
| Skippy.net -- WP-DB Backup Plugin for Wordpress | Directory traversal vulnerability in wp-db-backup.php in Skippy WP-DB-Backup plugin for WordPress 1.7 and earlier allows remote authenticated users with administrative privileges to read arbitrary files via a .. (dot dot) in the backup parameter to edit.php. | unknown<br>2006-08-17 | 2.3 | CVE-2006-4208<br>BUGTRAQ<br>OTHER-REF<br>OTHER-REF<br>BID<br>FRSIRT<br>SECUNIA<br>XF |
| SmartLine -- DeviceLock | SmartLine DeviceLock before 5.73 Build 305 does not properly enforce access control lists (ACL) in raw mode, which allows local users to bypass NTFS controls and obtain sensitive information. | unknown<br>2006-08-16 | 2.3 | CVE-2006-4184<br>BUGTRAQ<br>OTHER-REF<br>BID<br>SECUNIA<br>XF |
| Spidey Blog -- Spidey Blog Script | SQL injection vulnerability in proje_goster.php in Spidey Blog Script 1.5 and earlier allows remote attackers to execute arbitrary SQL commands via the pid parameter. | unknown<br>2006-08-17 | 2.3 | CVE-2006-4202<br>Milw0rm<br>BID<br>SECUNIA |

| | | | | |
|---|---|---|---|---|
| Sun -- Solaris | The squeue_drain function in Sun Solaris 10, possibly only when run on CMT processors, allows remote attackers to cause a denial of service ("bad trap" and system panic) by opening and closing a large number of TCP connections ("heavy TCP/IP loads"). NOTE: the original report specifies the function name as "drain_squeue," but this is likely incorrect. | unknown<br>2006-08-14 | 2.7 | CVE-2006-4117<br>SUNALERT<br>FRSIRT<br>SECUNIA |
| Sun -- Solaris | Race condition in Sun Solaris 10 allows attackers to cause a denial of service (system panic) via unspecified vectors related to ifconfig and either netstat or SNMP queries. | unknown<br>2006-08-14 | 2.7 | CVE-2006-4139<br>SUNALERT<br>FRSIRT<br>SECTRACK<br>SECUNIA |
| Webligo -- BlogHoster | Cross-site scripting (XSS) vulnerability in Webligo BlogHoster 2.2 allows remote attackers to inject arbitrary web script or HTML via the "From: part of the comment post," probably involving the nickname parameter to previewcomment.php. | unknown<br>2006-08-11 | 2.3 | CVE-2006-4090<br>BUGTRAQ<br>BID<br>FRSIRT<br>OSVDB<br>SECUNIA<br>XF |
| XennoBB -- XennoBB | Directory traversal vulnerability in the avatar_gallery action in profile.php in XennoBB 2.1.0 and earlier allows remote attackers to read arbitrary files via a .. (dot dot) in the category parameter. | unknown<br>2006-08-16 | 2.3 | CVE-2006-4161<br>BUGTRAQ<br>OTHER-REF<br>BID<br>SECUNIA<br>XF |

Back to top

**Last updated August 21, 2006**